

# 5. How can you navigate Nessus's user interface, including the dashboard and menus?

## Navigating Nessus's User Interface Like a Pro

Nessus has a **user-friendly web interface** that helps you **manage scans**, **analyze vulnerabilities**, and **generate reports** effectively. Below is a complete guide to navigating the dashboard and menus.

### ◆ 1. Accessing the Nessus Web Interface






#### Step 1: Open Nessus in Your Browser

- **URL:** `https://localhost:8834`
- **Login Credentials:** Use your **admin** username and password.

### ◆ 2. Understanding the Nessus Dashboard

Once logged in, you'll see the **Nessus Dashboard**, which provides an **overview of your security posture**.






#### Key Dashboard Sections:

| Section  | Description  |
|--|--|
|  <b>Scan Summary</b>                        | Shows completed scans, running scans, and schedules.               |
|  <b>Critical &amp; High Vulnerabilities</b> | Displays a summary of detected vulnerabilities ranked by severity. |
|  <b>Agent &amp; Plugin Updates</b>          | Ensures your Nessus installation is up to date.                    |
|  <b>Trending Vulnerabilities</b>            | Identifies new threats appearing in recent scans.                  |
|  <b>Target Assets</b>                       | Lists the most frequently scanned hosts and networks.              |

### ◆ 3. Navigating Nessus's Menus

Nessus has **five main menus** that help you control scans, policies, and reports.

#### Overview of Nessus's Main Menus

| Menu   | Function  |
|--|---|
|  <b>Dashboard</b> | Displays security insights, scan results, and vulnerability trends. |
|  <b>Scans</b>     | Manage, create, and schedule vulnerability scans.                   |
|  <b>Policies</b>  | Configure scan policies for optimal performance.                    |
|  <b>Plugins</b>   | Enable/disable vulnerability detection features.                    |
|  <b>Reports</b>   | Export detailed security assessments.                               |

---

## ◆ 4. Managing and Running Scans

Scans are the **heart of Nessus**, used to detect security vulnerabilities across your network.

### Steps to Create a New Scan

- 1 Click "Scans" > "New Scan"
- 2 Choose a scan template, such as:
  - ◆ **Basic Network Scan** (general vulnerability scan)
  - ◆ **Advanced Scan** (customizable settings)
  - ◆ **Web Application Scan** (for testing web security)
- 3 Enter **scan name, target IP addresses, or domains**.
- 4 Go to "Settings", optimize scan speed, and add credentials.
- 5 Click "Launch" to start scanning.

✓ **Pro Tip:** Use **scheduled scans** to automate routine security checks.

---

## ◆ 5. Reviewing Scan Results

### Steps to Analyze Vulnerabilities

- 1 Go to "Scans" > Click on a Completed Scan
- 2 The results will show:
  - 🚨 **Critical Vulnerabilities (Red)** → Urgent security risks
  - 🟠 **High Vulnerabilities (Orange)** → Serious issues
  - 🟡 **Medium Vulnerabilities (Yellow)** → Moderate risk
  - 🔵 **Low & Informational (Blue/Gray)** → Minimal impact
- 3 Click on any vulnerability to see:
  - **CVE ID** (Common Vulnerability Enumeration)
  - **Exploitability** (e.g., can it be exploited remotely?)

- **Affected Systems**
- **Recommended Fixes**

✓ **Pro Tip:** Export reports in **PDF, CSV, or JSON** for documentation.

---

## ◆ **6. Configuring Scan Policies**

**Policies** define how Nessus scans a target system.

### 🔧 **Steps to Create a Custom Policy**

- 1 Go to **"Policies" > "New Policy"**
- 2 Choose a scan type (e.g., **Basic, Advanced, Compliance**)
- 3 Adjust **Scan Performance** settings:
  - Increase **Max Simultaneous Hosts** for faster scanning
  - Enable **Safe Checks** to avoid crashing production systems
  - 4 Enable **credentialed scanning** for deeper security analysis
  - 5 Save and **apply the policy to new scans**

---

## ◆ **7. Managing Plugins**

Plugins power Nessus's ability to detect vulnerabilities.

### 🔧 **How to Enable/Disable Plugins**

- 1 Go to **"Settings" > "Plugins"**
- 2 Search for specific plugins (e.g., **Log4Shell, RCE, XSS**)
- 3 Enable/disable plugins to customize scans
- 4 Click **"Update Plugins"** regularly to stay protected

✓ **Pro Tip:** Disable unnecessary plugins to **reduce scan time**.

---

## ◆ **8. Exporting & Automating Reports**

Reports help you **document findings and track security improvements**.

### 🔧 **How to Generate a Report**

- 1 Go to **"Reports" > Select a Scan**
- 2 Click **"Export"**, then choose:
  - 📄 **PDF** (for management reports)
  - 🇮🇹 **CSV** (for raw data analysis)

- 📄 **JSON/XML** (for API integrations)
  - 3 Automate reporting by **scheduling exports**

✓ **Pro Tip:** Integrate Nessus with **SIEM tools like Splunk** for real-time monitoring.

---

## ◆ 9. Configuring User Roles & Access Control

Manage user access to **restrict unauthorized changes**.

### 🔧 Steps to Add & Configure Users

- 1 Go to "Settings" > "Users"
  - 2 Click "Add User", then choose:
    - **Administrator** → Full control over Nessus
    - **Standard User** → Can run scans but not modify policies
    - **Read-Only User** → View reports only
- 3 Enable **Two-Factor Authentication (2FA)** for added security
  - 4 Save settings & assign users to appropriate roles

✓ **Pro Tip:** Use **RBAC (Role-Based Access Control)** to prevent unauthorized scans.

---

## 🎯 Final Tips for Mastering Nessus UI

- ✓ **Use the Dashboard Daily** → Monitor security trends in real-time
- ✓ **Customize Scan Policies** → Optimize for speed & accuracy
- ✓ **Use Credentialed Scans** → Get deeper insights with lower false positives
- ✓ **Leverage Plugin Management** → Disable what you don't need to speed up scans
- ✓ **Automate Reports** → Save time and keep security teams updated